University of New South Wales Law Research Series

INDIA'S DATA PRIVACY BILL: PROGRESSIVE PRINCIPLES, UNCERTAIN ENFORCEABILITY

GRAHAM GREENLEAF

[2020] *UNSWLRS* 38

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

India's data privacy Bill: Progressive principles, uncertain enforceability

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
(2020) 163 *Privacy Laws & Business International Report* 1, 6-9

India's Modi government has at long last submitted the *Personal Data Protection Bill, 2019*[1] to India's lower house, the Lok Sabha. The government Bill is based on the draft Bill (and Report[2]) prepared by the committee chaired by former Supreme Court Justice Srikrishna, but almost every clause of the 'Srikrishna Bill' is varied by this Bill. Nevertheless, the structure of Srikrishna Bill, including its many influences from the EU's GDPR, is largely retained. The Bill has now been referred to a Joint Parliamentary Committee of both Houses, which has called for submissions on the Bill by 25 February 2020, and may take some oral evidence.[3]

The Indian government has compelling reasons to enact such a Bill, both to protect legislation and practices on which government programs depend against findings of unconstitutionality because of inadequate protection of privacy,[4] and in order to maximize India's prospects of obtaining a positive 'adequacy assessment' from the European Union under the GDPR. The Srikrishna Report provides cogent arguments from a policy perspective why a strong Bill is in the interests of the Indian people and Indian businesses and government. The government Bill gives India prospects of achieving both objectives, but only if some changes are made to the Bill.

This article aims to provide a critical overview of the main elements of the government Bill ('the Bill'), with an emphasis on significant differences from the Srikrishna Bill, and on comparisons with the EU's GDPR.[5] Some additional criticisms are elaborated in my submission to the Joint Parliamentary Committee.[6]

The Bill uses some unusual, but appropriate, terminology: data subjects are referred to as 'data principals'; and data controllers are referred to as 'data fiduciaries'.

Scope

The Bill's scope is comprehensive covering both the public and private sectors, where personal data is processed within India, or by Indian companies, citizens or bodies created under Indian law, no matter where located (s. 2). It also has extra-territorial application very

[1] Personal Data Protection Bill, 2019 (India) <https://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf>

[2] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* < http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf >

[3] Lok Sabha Secretariat Press Communique 'Joint Committee on the Personal Data Protection Bill 2019' 22 January 2020 <https://twitter.com/LokSabhaSectt/status/1220636832561369089>.

[4] Indians have an 'inalienable and inherent' constitutional rights of privacy following the Supreme Court decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* 2017 (10) SCALE 1 (*Puttaswamy #1).*

[5] Some of these criticisms are the same as I made about the Srikrishna Bill in 'GDPR-Lite and requiring strengthening – Submission on the draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)', 20 September 2018 < https://papers.ssrn.com/abstract_id=3252286 >.

[6] G. Greenleaf, Graham, India's Personal Data Protection Bill, 2019 needs closer adherence to global standards (Submission to Joint Committee, Parliament of India) (12 February 2020). < https://ssrn.com/abstract=3539432>

similar to the GDPR (s. 2(A)(c)), which will help establish this as a new standard for data privacy laws.

A major exception to its scope is the government's powers to exempt, by executive order, 'any agency of the government' from any provisions of the Bill for any type of processing, on a very wide variety of grounds (s. 35). In contrast, the Srikrishna Bill limited such exemptions to grounds of State security, by legislation made by Parliament, and only where necessary and proportionate to the objective to be achieved (s. 42 Srikrishna Bill). It has been argued that s. 35 would be inconsistent with India's constitutional right of privacy, because it fails the tests set out in *Puttaswamy #1* for legislative interferences with that right.[7]

Also undesirable - if India wishes to be seen as a global leader in the ethical processing of personal data - is the Government power to exempt specified processing of personal data of foreign nationals not present in India (the 'outsourcing exemption') (s. 104). The EU would need to insist, as part of any adequacy discussions, that this provision does not apply to EU-origin personal data.

A complex data protection authority

Central to the Bill, because it has so much power, is the creation of the Data Protection Authority of India (DPAI), and the related roles of Adjudicating Officers (AOs) and the Appellate Tribunal in settling disputes. Data Protection Officers (DPOs) and Auditors also have distinct roles. Overall, this is a complex new form of administrative and enforcement structure for data privacy, which needs explanation before rights and obligations are discussed.

Data Protection Authority of India (DPAI)

The DPAI, consisting of a Chairperson and up to six full-time Members, is described by the Srikrishna Report as an 'independent regulatory body', but is not despite the fact that it regulates government. DPIA Members are public servants (s. 87), and there is no explicit statement that the DPAI must act independently. To the contrary, the Government can issue directions to it, as it thinks fit, to protect a range of high state interests; and it is bound in exercising its functions by any written directions from the government 'on questions of policy' (on which classification the government's decision is purportedly final) (s. 86). Such directions are not required to be made public.

DPAI inquiries and Adjudicating Officers (AOs)

The DPAI may commence an inquiry, either on its own initiative ('suo moto'), or on the basis of a complaint received, (s. 53). It empowers one of its officers as an Inquiry Officer, to investigate and report to it. The DPAI is then able to issue warnings, reprimands, and orders that any actions be taken or discontinued by the data fiduciary or processor (s. 54). These respondents have a right of appeal to the Appellate Tribunal (s. 54(2)), but data principals do not have an explicit right of appeal, and would have to rely on being a 'person aggrieved' by a DPAI decision in order to appeal under s. 72(1). DPAI orders do not include requiring any monetary payments, either fines or compensation.

The DPAI is to appoint Adjudicating Officers (AOs), with requirements of independence,[8] who will decide penalties (fines) and compensation payable (s. 62(1)). Penalties (fines) can only

[7] As discussed in detail in Dvara Research *Initial Comments ... on the Personal Data Protection Bill'* 16 January 2020, pp. 10-13 <https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf >.

[8] For details, see Greenleaf *Submission to Joint Committee*.

be imposed by AOs, following (i) the DPAI making a complaint to an AO; (ii) the AO giving the respondent a hearing; and (iii) the AO is satisfied that the respondent has contravened the Act or caused harm to a data principal as a result of such a contravention (s. 63). Once a contravention has been established, the AO is required to consider a list of factors relevant to the seriousness of the contravention, in decided whether to impose a penalty, and the quantum (s. 63(4)). Either party may appeal to the Appellate Tribunal. The maximum penalties for substantive breaches of the Act's principles are 15 crore rupees (US$2.1 million) or 4% of total worldwide turnover in the previous financial year (s. 58(2)), whichever is the greater. For breaches of administrative requirements of the Act, the equivalent maxima are 5 crore rupees (US$705.000) and 2% (s. 58(1)). These potential penalties meet the highest global standards, as set by the EU's GDPR.

The Bill is unusual in providing for a data protection authority to order compensation payments. Where a data principal 'has suffered harm' (defined in s. 3(20), but only by examples) as a result of any contravention of the Act, rules or regulations, by a data fiduciary or data processor, they may seek compensation by making a complaint to the AO (s. 64). The AO must take into account a set of factors relevant to the extent of harm, and the culpability of the respondent, including their previous history of contraventions (s. 64(4)). Either party may appeal to the Appellate Tribunal (s. 64(7)). No limit is placed on the amount of compensation that may be ordered.

NGOs and litigation

Joint actions by an 'identifiable class' who have suffered harm may be commenced for compensation (s. 64(3)). However, there is no explicit provision empowering NGOs specialising in privacy to make complaints in order to initiate enforcement actions seeking orders, or penalties, unlike in GDPR art. 80.

Appellate Tribunal

The government is to establish an Appellate Tribunal to hear appeals from the decisions of both the DPAI and AOs (s.67). It can appoint an existing body to act as such a tribunal (s. 67(4)). Further appeals can be made to the Supreme Court, but only 'on any substantial question of law' (s. 75), not on questions of fact.

Varieties of personal data

The Bill has a conventional definition of 'personal data' based on direct or indirect identifiability (s. 3(26)), but has some unusual provisions concerning both sensitive personal data and anonymous data.

Sensitive personal data'

The definition of 'sensitive personal data' (s. 3(36)) is unusual because it includes 'financial data' (largely limited to account identifiers, and data concerning relationships with financial institutions: s 3(18)). The definition excludes racial or ethnic origin (while including 'caste or tribe'), trade union membership, and criminal records. 'Biometric data' (s. 3(7)) and 'genetic data' (s. 3(19)) are both included and defined broadly. The government, after consulting the DPAI and any other relevant regulators, can by notification expand the categories of sensitive personal data (s. 15(1)).

Important aspects of the Bill concerning data localisation and exports depend on whether data is or is not sensitive personal data. Most data privacy laws specify higher standards of protection for sensitive personal data, but this Bill does not, leaving it to the DPAI to specify by regulations such additional protections as may be needed (s. 15(2)). This was also a

deficiency of the Srikrishna Bill, and is a considerable difference between these Bills and the GDPR.

'Anonymisation' demarcates when information is no longer personal data (s. 2(B)), but the Bill is ambiguous whether compliance with a standard of anonymisation set by the DPAI will not be able to be challenged by expert evidence of irreversibility in light of current knowledge, which may present adequacy problems.[9]

Obligations of 'data fiduciaries', and rights of data principals

A novel aspect of the Bill is that it creates what are in effect three categories of data fiduciaries, with differing obligations:

'**Significant data fiduciaries'** (SDFs) are data fiduciaries designated (individually or as a class) by the DPAI, based on six criteria of 'significance', particularly the 'risk of harm' of their processing (s. 26(1)). SDFs have additional obligations (see below), not imposed on other fiduciaries. There are special provisions for a 'social media intermediary' to be designated as a SDF (s. 26(4)).

'**Small entities'** (SEs) that only do manual processing of personal data are exempt from many obligations (s. 39(1)). A 'small entity' is to be determined by regulations based on annual turnover (it was specified as less than US$30K p/a in the Srikrishna Bill), volume of data processed, and purpose of processing.

'Normal' data fiduciaries are therefore those without the additional obligations of a significant data fiduciary, but without the reduced obligations of a small entity. However, the DPAI can require a class of 'normal' data fiduciaries to have some SDF obligations: s26(3).

Differing obligations of categories of data fiduciaries

The main obligations of data fiduciaries (including to observe rights of data principals) are listed below, noting which only apply to SDFs ('SDF only') and which do not apply to 'small entities' ('SE exempt').

Rights of data principals (obligations of normal and significant data fiduciaries):

- *Access* rights, may be limited to access to a 'brief summary' of personal data, and of processing activities (s. 17), instead of guaranteeing access to 'a copy' of both (SE partly exempt).
- *Correction, completion and updating* (s. 18(1)), including informing third party recipients (s. 18(4)).
- Data *portability* (s. 19), including data generated or added by the data fiduciary (may be stronger than the GDPR) (SE exempt).
- *Right to be forgotten* (RTBF), through erasure or restricting disclosure, where processing is no longer necessary (s. 18(1)(d) and s. 20(1)(a)) (SE partly exempt).
- *Right to restrict continuing disclosure* based on withdrawal of consent or processing illegal, but only if an AO so orders (s. 20(1)(b) and (c)) (SE exempt).

Obligations of 'normal' data fiduciaries and SDFs:

- *Minimisation* of data collection (s. 6, s.11(4)).

[9] For other anonymisation issues, see Greenleaf *Submission to Joint Committee*.

- *Notice obligations* (extensive) for collection from data principals, or from third parties (s. 7) (SE exempt).
- *Data quality* obligations, including requirement to notify third party recipients of changes (s. 8) (SE exempt).
- Automatic *deletion* when purpose complete (s. 9) (SE exempt).
- Data fiduciary *responsible for processors* (s.10), and requirements for contracts (s. 31).
- *'Privacy by design' policy* required (s. 22), but not implementation (SE exempt).
- *Transparency* of specified information (s. 23), with additional notice obligations, and a specified role for 'consent managers' (SE exempt).
- *Security safeguards*, including periodic review as specified (s. 24) (SE exempt).
- *Data breach notification* to the DPAI (s. 25), and to data principals but only at the discretion of DPAI, with no objective criteria requiring notification (s. 25(5)) (SE exempt).
- *Grievance redressal mechanism* required (s. 32) (SE exempt).

Increased obligations of 'significant data fiduciaries', 'SDF only' unless DPAI specifies:

- *Registration* with DPAI, as it specifies (s. 26(2)).
- *Data protection impact assessment* before processing commences (DPIA) required by SDFs where there is a significant risk of harm, and mandatory where DPAI specifies, that a processing is submitted to DPAI for directions (s. 27).
- *Record-keeping* required (s. 28), sufficient to demonstrate compliance, document security reviews, DPIAs, plus others as DPAI specifies, and includes all government entities.
- *Auditors,* independent and registered with DPAI required annually (or when DPAI demands), with auditors assigning a rating ('data trust score') (s. 29).
- *Data Protection Officer* (DPO) required to be appointed, with tasks specified, and DPAI-specified qualifications (s. 30).

The differing scopes of applicability of the Bill's obligations will raise questions requiring consideration in an EU adequacy assessment. Some rights that are found in the GDPR were not adopted in the Srikrishna Report and Bill, and they are also absent from this Bill.[10]

Grounds for lawful processing

The EU influence on this legislation is most clearly shown in that all processing of personal data must have a lawful basis (ss. 11-14). The ground of consent of the data principal requires a high standard of consent for it to be valid (s. 11). A non-consensual ground for various government and emergency uses (s. 12), and employment uses (s. 13), are specified, but only apply to non-sensitive data. The DPAI can specify by regulations a broad range of 'reasonable purposes' as grounds for non-consensual processing of any personal data (s. 14), with factors it must consider, a requirement to include appropriate safeguards, and a list of possible examples of 'reasonable purposes', but with no real limits on the subject matter the DPAI can include. The Srikrishna Bill limited the DPAI's power to specific lawful grounds by regulation to non-sensitive information, but that limit has been abandoned.

Cross-border exports, and data localisation

India's approach to limits on the export of personal data is very unusual. In effect, it divides personal data into four categories, with major differences in the treatment of sensitive and

[10] For details, see Greenleaf *Submission to Joint Committee*.

non-sensitive personal data (ss. 33-34). Three types of 'data localisation' result, which can only be summarised here:[11]

(1) *Local copy requirements* (localisation #1): All sensitive personal data must be stored in India', whether or not it is allowed to be exported.
(2) *Export requirements* (localisation #2) allow sensitive personal data be transferred outside India in four situations: (a) explicit consent of data principal; (b) transfers pursuant to contract or inter-group scheme approved by the DPAI, with exporter remaining liable; (c) transfers to a country, class of entities etc which the government has found provides adequate protection; (d) DPAI has allowed transfers 'for any specific purpose'.
(3) *Export prohibitions on critical personal data* (CPD – defined by government) (localisation #3), unless exempted for emergency medical purposes, or adequate and also has government approval in the particular case.
(4) *Non-sensitive personal data* has no restrictions on export, no local storage requirements, unless deemed to be CPD under 3) above.

These complex provisions give the government and the DPAI a great deal of discretionary control, with few legislative constraints. A more conservative and legally constrained approach is desirable.

Conclusions

The Modi government's Bill includes, at least superficially, a large proportion of the rights and obligations found in leading international data privacy standards, particularly the GDPR. In this respect it is similar to the Srikrishna Bill, although it weakens some principles. The penalties for breaches of the law, and the compensation provisions are also superficially strong, well up to international standards. In these respects, it is a progressive Bill.

However, when it comes to questions of whether it is likely to be enforced strongly and effectively, this Bill falls well short of international standards. The DPAI is dominated by government appointments, and lacks guarantees of independence. Data principals (and NGOs representing them) lack sufficient independent abilities to take enforcement action. The scope for the government to exempt public sector bodies from the law is far too broad.

This Bill goes even further than the Srikrishna Bill in implementing a very different regulatory philosophy from the EU GDPR's radical dispersal of decision-making responsibility (and liability for wrong decisions) to data controllers. The Indian model is more prescriptive (perhaps closer to the 1995 EU Directive in this respect), but it is implemented in section after section by leaving the essential regulatory details to be completed by the Data Protection Authority of India (DPAI), or the Indian government, through delegated legislation. Until these regulations are completed, the result will a high degree of uncertainty as to how much protection the Bill will offer data principals, and a long period of uncertainty impeding planning by Indian businesses.

.

[11] For details, see Greenleaf *Submission to Joint Committee*.